(1) 25

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 January 2002 (17.01.2002)

PCT

(10) International Publication Number
WO 02/05514 A1

(51) International Patent Classification[7]: H04L 29/06, H04Q 11/04

(21) International Application Number: PCT/SE01/01590

(22) International Filing Date: 6 July 2001 (06.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0002586-6 7 July 2000 (07.07.2000) SE

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SÖDERBERG, Johan** [SE/SE]; Docentvägen 14, S-977 52 Luleå (SE). **HEDLUND, Mikael** [SE/SE]; Sandviksgatan 25, S-972 38 Luleå (SE).

(74) Agent: **MAGNUSSON, Monica**; Ericsson Radio Systems AB, Patent Unit Radio Access, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

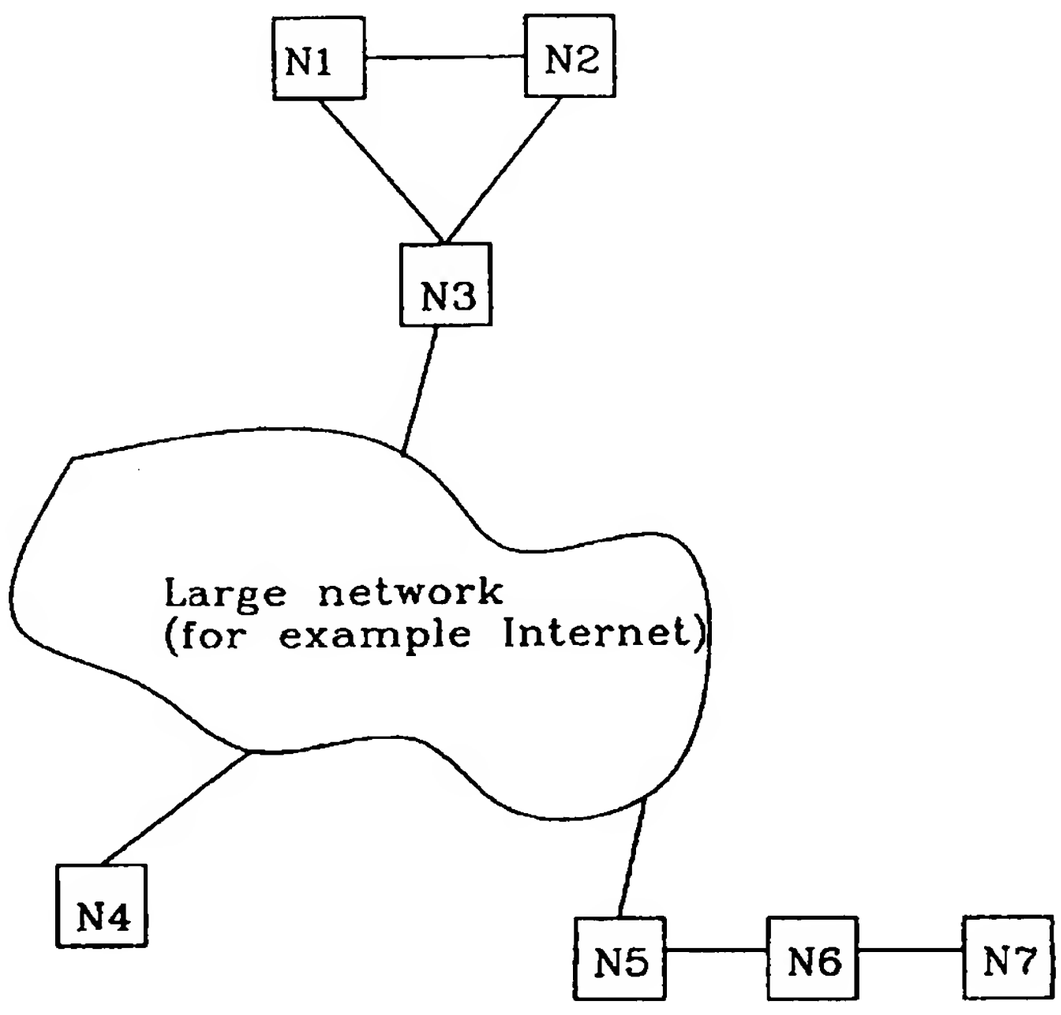
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD AND AN ARRANGEMENT RELATING TO COMMUNICAITONS SYSTEMS

(57) Abstract: The present invention relates to a method of blocking undesired traffic in data communication systems that uses packet switching. Blocking is effected by determining the sender address of incoming data packets, and then comparing this address with a list of reliable addresses. The data packet is erased immediately, if the sender addresss is not included in the list. The list of accepted addresses can be created in several wayoi among others by including in the list addresses to which the user has himself sent data, these addresses therefore being considered reliable addresses. Addresses of friends and acquaintances can also be inserted in the list manually. The invetion thus enables undesired data from unreliable senders to be avoided. Such data loading limited resources, such as wireless internet connections for example. Neither is there any risk of the receiver being required to pay for information that he himself has not requested.



WO 02/05514 A1

A METHOD AND AN ARRANGEMENT RELATING TO COMMUNICATIONS SYSTEMS

FIELD OF INVENTION

The present invention relates to the field of data communications systems. More specifically, the invention relates to a method of blocking undesired traffic in a data communications system.

The invention relates particularly, but not exclusively, to a method of blocking undesired data packets that are sent on a network which uses packet switching and where the network protocol is preferably represented by Internet Protocol (IP).

The invention can be applied on both wireless communications systems, for instance GPRS and WCDMA, and traditional so-called fixed communications systems constructed by fibre cables for instance.

DESCRIPTION OF THE BACKGROUND ART

In a packet-switching data communications system information is sent in packets, wherein each packet travels over the network with the best of efforts with respect to speed and routing, as opposed to a circuit switched network in which a connection is set up and all information sent precisely in accordance with the pre-established route.

In packet switching networks, the data packet utilises addresses in order to reach its final destination, in other words each packet is marked with a terminal address and the packets then dispatched. The network then ensures that the packets arrive at the correct receiver. Each packet will normally also include a sender address, so that the sender of the packet will be known.

Thus, information can be sent in a packet switched network at any time whatsoever and to all nodes that are connected to the network, without first contacting the receiver.

It is known, for instance from PCT-application WO9826533, to filter data packets by to data packets an attribute which indicates whether the receipt of the packets is desired or undesired. This attribute may be the address of the sender of the packet.

SUMMARY OF THE INVENTION

One problem with packet switching network is that whosoever can send whatsoever to whomsoever. The data packet is forwarded in the network without first checking whether or not the receiver will actually have the information. This does not occur in circuits switched communications systems in which there is first set up a connection between two parties. This can result in a user being drowned in a large quantity of undesired data that loads a resource-limited system unnecessarily.

When payment is expected for the amount of data received, another problem is that whosoever can cause an economic injury by sending the data packet to a user who is then forced to pay for the receipt of undesired and worthless information.

Thus, the object of the present invention is to provide a solution to the aforesaid problems. In brief, this object is realised by believing that each terminal address to which data is sent, for example an e- mail receiver or in response to a request on a web page, is considered to be reliable. Data is then accepted solely from these accepted addresses, i.e. from reliable senders, and all other data packets are discarded.

More specifically, the checking and filtering of data packets is normally effected automatically. A list of accepted senders is created automatically, by investigating the terminal address of outgoing packets and placing this address in the list. A user

may also insert beforehand addresses from which he is willing to receive data packets. The sender address of respective incoming packets is then compared with the addresses on the list. The invention can be applied in any network node whatsoever.

One advantage afforded by the invention is that one avoids receiving undesired data from unknown or unreliable senders.

Another advantage is that there is no risk of being required to pay for information that has not been requested.

The invention will now be described in more detail with reference to preferred exemplifying embodiments thereof and also with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows parts of a packet switching network.

Figure 2 illustrates the various link layers in the OSI-model.

Figure 3 shows an IP-header for IP-version 4.

Figure 4 shows a TCP-header.

Figure 5 illustrates how the three-way handshake algorithm functions.

Figure 6 is a flow chart for outgoing packets according to one embodiment of the invention.

Figure 7 is a flow chart for incoming packets according to one embodiment of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 shows the possible configuration of parts of a packet switching network. The example shows how several nodes (N1, N2, N3...) are interlinked in one or more networks. For example, the nodes N1-N3 and N5-N7 may form two separate small networks which, in turn, are coupled together with a larger network, for instance with Internet. Each small network can use different types of technology, for example FDDI, Ethernet or ATM. In Figure 2, the nodes N1-N3 might be able to use ATM within their small network, whereas the nodes N5-N7 might be able to use Ethernet within their small network.

When these smaller data networks are coupled together, there is created a larger data network. Thus, Internet is actually a logic network that consists of a collection of physical networks, i.e. a collection of smaller networks that use different technologies.

These smaller networks are coupled together with the aid of routers and gateways. A router ensures that data packets are sent along correct routes between the networks, whereas a gateway manages the communication between different types of protocols, for instance so that an ATM-network is able to communicate with an Ethernet-network.

The OSI-model shown in Figure 2 describes the various layers that are included in a packet switching communications system. The bottom Layer 1 is the physical layer that specifies transportation of bits over the physical medium. V.24, V.34 and G.703 are examples of Layer 1 standards.

There then follows Layer 2 which is the data link layer that specifies frames and physical addresses. Ethernet, Token Ring and High level Data Link Control (HDLC) are examples of Layer 2 standards. Layer 3 is the network layer that manages routing, logic addresses and data packet fragmentation. Internet Protocol (IP) and Internetwork Packet Exchange (IPX) are possible examples in this regard.

These three lowermost Layers 1-3 are, as shown in Figure 2, implemented in all network nodes, including network switches and all nodes coupled along said networks.

Layer 4 is the transport layer that is normally implemented solely in the end nodes. User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) are examples of protocols in the transport layer.

Layer 5 is the sessions layer that, inter alia, checks that the session has not been terminated before all data has been transmitted. Examples in this regard may be netbios and winsock.

Layer 6 is the presentation layer that specifies coding of data. HyperText Marup Language (HTML) and American Standard Code for Information Interchange (ASCII) are examples in this regard.

The top Layer 7 is where the actual applications are implemented, such as e-mail and file transfers. Examples in this regard are telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMPT) and HyperText Transport Protocol (HTTP).

Figure 3 illustrates the construction of an IP-header for IP-version 4. An Ipv4 header consists of several 32-bit words. The first word includes Version which indicates the version of IP used. Hlen indicates the length of the entire header. TOS (Type Of

Service) is conceived for use for extra services, for instance giving priority to faster transportation.

The field Protocol concerns which higher-layer protocol manages the IP-packet, examples of such protocol being TCP or UDP. This field is thus examined to see whether or not TCP was used, and therewith also examined to see whether or not SYN and ACK were sent, as is carried out in one embodiment of the invention.

A checksum is a sum that is calculated by discerning the whole of the IP-header as a number of mutually summated 16-bit words. If this field does not agree with the computation carried out upon arrival of the packet, the packet is discarded.

The SourceAddress reveals the address from which the packet is sent, i.e. the origin of the packet, this being required in order to be able to reply to a message. The address of origin may, for instance, be an IP-address, such as 130.240.193.75.

The DestinationAddress reveals the address to which the packet shall be sent, in other words the terminal address. This address is used by each router in making a decision and determining the route along which the packet shall be forwarded in the network. The receiver address may, for instance, be an IP-address, such as 136.225.151.252. When IP is used in conjunction with the invention, it is this field together with the aforesaid source address field that is used to ascertain whether or not the data packet shall be accepted.

Although options is not normally used, it can, however, be used to indicate a particular route through the network, and Data is the actual payload data that may consist of the subject matter to the dispatch, for instance, text, pictures or speech.

Figure 4 shows the construction of a TCP-header. The TCP-header also consists of several 32-bit words. The first field SrcPort indicates the port that was used in the

node from which the packet was sent. DstPort denotes the corresponding port in the node to which the packet shall be sent. Because TCP is a byte-orientated protocol, each byte of data will have a sequence number, which is given by SeqNo. Acknowledgement indicates which sequence is next in line, i.e. the sequence number accepted next by the receiver. HdrL denotes the length of the header.

In the field Flags, which consists of 6 bits, the content of the packet is disclosed in slightly more detail, where the bit order is as follows: URG-ACK-PUSH-RESET-SYN-FIN, wherewith each bit has the following connotation:

URG which is a flag for urgent data conceived for use in signalling important messages concerning traffic;

The ACK-bit (010000 in Flags), which is the flag that states whether or not valid information is found in the Acknowledgement field;

PUSH, which is used when wishing to send collected data directly, without waiting to fill a complete packet, PUSH being used for instance, in telnet where each written character is sent directly;

RESET which indicates that the receiver of data has obtained erroneous information, for instance an unexpected segment with the wrong sequence number or the wrong Checksum, and therewith wishes to terminate the connection;

SYN-bit (000010 in Flags), which are used when establishing a TCP-connection; and

FIN, which is used when a connection shall be terminated.

AdvWindow indicates the size of the transmission window used, i.e. how much data is sent before a receiving acknowledgement can be expected. Checksum is a sum that is calculated by summating the contents of the header, so as to ascertain whether or not this content is in agreement with the received content. UrgPtr indicates the number of bytes of urgent data (if URG is placed in Flags). TCP-choice can be specified in options, and the Data-field is the payload data sent.

Figure 5 is a schematic image of the so-called three way handshake algorithm used by TCP for establishing a connection. The client commences by sending to the server a segment, (Flags = SYN, SeqNo=x) that indicates which sequence number the client intends to use. The server then responds with an acknowlegement (Flags = ACK, SeqNo=y) of the client's sequence number and an own sequence number (Flags = SYN, Ack=x+1) that the server intends to use. Finally, the client responds with a third segment (ACK, Ack=y+1) that confirms the server's sequence number.

This algorithm is used between all end nodes that send data therebetween, regardless of whether it involves two clients, two servers, or one server and one client. Although the handshaking algorithm shown by way of example is for TCP, it will be understood that other handshake algorithms may alternatively be used in accordance with the invention, for instance a WAP handshake algorithm.

According to one embodiment of the invention, only SYN/ACK is studied in order to ascertain whether or not packets arriving from this session will be accepted. This reduces the number of outgoing packets that need to be checked. All that is required is to look when a connection is established, therewith obviating the need to check outgoing packets in said session. ?

Figures 1-5 now give a background that leads to the invention itself, i.e. how data packets are filtered. This is described below chiefly with reference to Figures 6 and 7.

Figure 6 is a flow chart for outgoing data packets in one embodiment of the invention. The first step 201 involves ascertaining whether or not data packets are affiliated with a handshake protocol. The second step 202 involves ascertaining whether or not an outgoing data packet belongs to a handshake procedure, which when TCP is used is shown, for instance, in the abovementioned field Flags, where SYN and/or

ACK may be given. These two steps can be carried out within the concept of the invention to reduce the number of outgoing data packets that shall be examined.

The third step 203 involves examining the destination address of the data packet, which, when Internet Protocol (IP) is used, can be found in the DestinationAddress of the IP-header, which states the address to which each data packet shall be sent.

The next step 204 involves finding the destination address of the outgoing data packet in the list of accepted addresses.

Step 205 is implemented when the response in the preceding step 204 is NEGATIVE, meaning that the address is not included in the list. The user is then asked whether or not the destination address of the outgoing data packet shall be included in the list.

Step 206 involves including the address in the list, if the user answers YES to the question.

Step 207 involves releasing the packet for transportation out in the network. This step can follow step 204, 205 or 206, depending on the answers given to the aforesaid questions and the result of the list scan, or whether or not automatic updating of the list shall be used instead of asking a question of the user in this regard.

Figure 7 is a flow chart for incoming data packets in one embodiment of the invention. The first step 100 involves examining the address of origin of the data packet. This can be seen, for instance, in the SourceAddress field of the IP-header when using Internet Protocol.

The next step 101 involves looking for the address in the list of accepted addresses.

Step 102 is carried out when the address cannot be found in the preceding step 101, meaning that the sender is unknown/not accepted.

The user is then asked whether or not he is willing to receive the data packet nevertheless.

Step 103 is carried out when the user states in the preceding step 102 that he does not wish to receive the packet. The packet will then be erased. Alternatively, this step is carried out immediately after step 101 when the address cannot be found and the user does not wish to ask this question for each unknown sender.

Step 104, which means that receipt of the packet in the node is avoided, may take place after several steps (101 or 102), depending on whether or not the address is found in the list or depending on the answer given to said question.

The list of accepted addresses of origin might include both addresses statically inserted in the list and addresses that are generated automatically. This enables a user to create the list beforehand or to update the list with accepted addresses of origin. Alternatively, the list can be created or updated automatically by including the addresses to which data packets are sent automatically in the list, in accordance with the invention.

The person applying the invention may, for instance, be a person who uses a wireless connection to the Internet, via node N4 in Figure 1. The user then sends an email to a user connected via node N6 in Figure 1, and requests home a number of web pages from Node N3. The user then considers the addresses of nodes N6 and N3 to be reliable. If a file is sent from a person who does not have one of the aforesaid addresses of origin, the file is erased before our person receives the file on his computer. Thus, in the case of this example, the invention can be implemented in a node upstream of our user, for instance in the penultimate node – which may be the

base station – prior to the file being sent to our user in a wireless node. This is done in order to save space on the limited bandwidth in the air interface.

It will be understood that the invention is not restricted to the aforedescribed and illustrated exemplifying embodiments thereof and that modifications can be made within the scope of the accompanying claim.

CLAIMS

1. A method of blocking undesired data traffic in a communications system that includes at least two nodes, wherein communication between said nodes takes place in a packet switching network, **characterised by** accepting from addresses of origin solely data packets that correspond to destination addresses to which the node concerned has, itself, sent said data packet.

2. A method according to Claim 1, **characterised by** the further steps with respect to incoming data packets of:
- determining (100) the address of origin of said data packet;
- comparing (101) the address of origin of the data packet with a list of accepted addresses of origin;
- allowing the data packet to pass through (104) when said packet has an accepted address of origin; or
- erasing (103) said data packet if its address of origin is not accepted.

3. A method according to Claim 2, **characterised by** preceding said erasion of the data packet with a question (102) asking whether the user is willing to receive the data packet from an unaccepted address of origin.

4. A method according to any one of Claims 1-3, **characterised in** that the method comprises the following steps with regard to outgoing data packets of:
- determining (203) the destination address of the data packet;
- comparing (204) the destination address with a list of accepted addresses of origin;
- allowing the packet to pass through (207) if said destination address is included; or
- adding (206) the destination address as an accepted address of origin to the list of accepted addresses of origin when said address is not included in said list, and then allowing the data packet to enter the network (207).

5. A method to Claim 4, **characterised by** preceding addition (206) of a destination address with a question (204) asking whether or not the user wishes to include the destination address as an accepted address of origin.

6. A method according to any one of Claims 4-5, **characterised by** carrying out the aforesaid steps (203-207) with respect to outgoing data packets solely during the handshake algorithm for establishing a connection, and preceding said steps by the following steps of:
- determining (201) whether or not an outgoing data packet belongs to a handshake protocol; and
- determining (202) whether or not an outgoing data packet is included in a handshake procedure.

7. A method according to any one of Claims 1-6, **characterised in** that the network protocol is comprised of Internet Protocol (IP).

8. A method according to Claim 7, **characterised in** that the transport protocol is comprised of the User Datagram Protocol (UDP).

9. A method according to Claim 7, **characterised in** that the transport protocol is the Transmission Control Protocol (TCP).

10. A method according to any one of Claims 1-9, **characterised in** that the communication system is comprised of a system of the type TDMA (Time Division Multiple Access) with packet data addition.

11. A method according to any one of Claims 1-9, **characterised in** that the communication system is a PDC (Personal Digital Cellular) type system.

12. A method according to any one of Claims 1-9, **characterised in** that the communication system is a WCDMA (Wideband Code Division Multiple Access) type system.

13. A method according to Claim 10, **characterised in** that the packet data addition is a GPRS (General Packed Radio Service).

14. A communications unit for blocking undesired data traffic in a communications system that includes at least two nodes, wherewith communication between said nodes takes place i a packet switch network, **characterised in** that the communications system includes means for accepting solely data packets that are sent from addresses of origin that correspond to destination addresses to which the communications unit concerned has itself sent said data packet.

15. A communications unit according to Claim 14, **characterised in** that the unit includes for incoming data packets means for determining the addresses of origin of said data packet, mans for comparing the addresses of origin with a list of accepted addresses, means for allowing a data packet that has an accepted address of origin to pass through, and means for erasing data packets that do not have an accepted address of origin.

16. A communications unit according to Claim 15, **characterised by** means for asking the user whether he/she is willing to receive a data packet from an unaccepted address of origin.

17. A communications unit according to any one of Claims 14-16, **characterised in** that for outgoing data packets said unit further includes means for determining data packet destination addresses, means for comparing destination addresses with a list of accepted addresses of origin, means for allowing a data packet whose destination

address is included in said list to pass through, and means for adding destination addresses to the list when said list does not include said destination addresses.

18. A communications unit according to Claim 17, **characterised by** means for asking the user whether or not he/she wishes to include a destination address to the list.

19. A communications unit according to any one of Claims 17-18, **characterised by** means for determining whether or not outgoing data packets belong to a handshake protocol, and by means for determining whether or not said outgoing data packets are included in a handshake procedure.

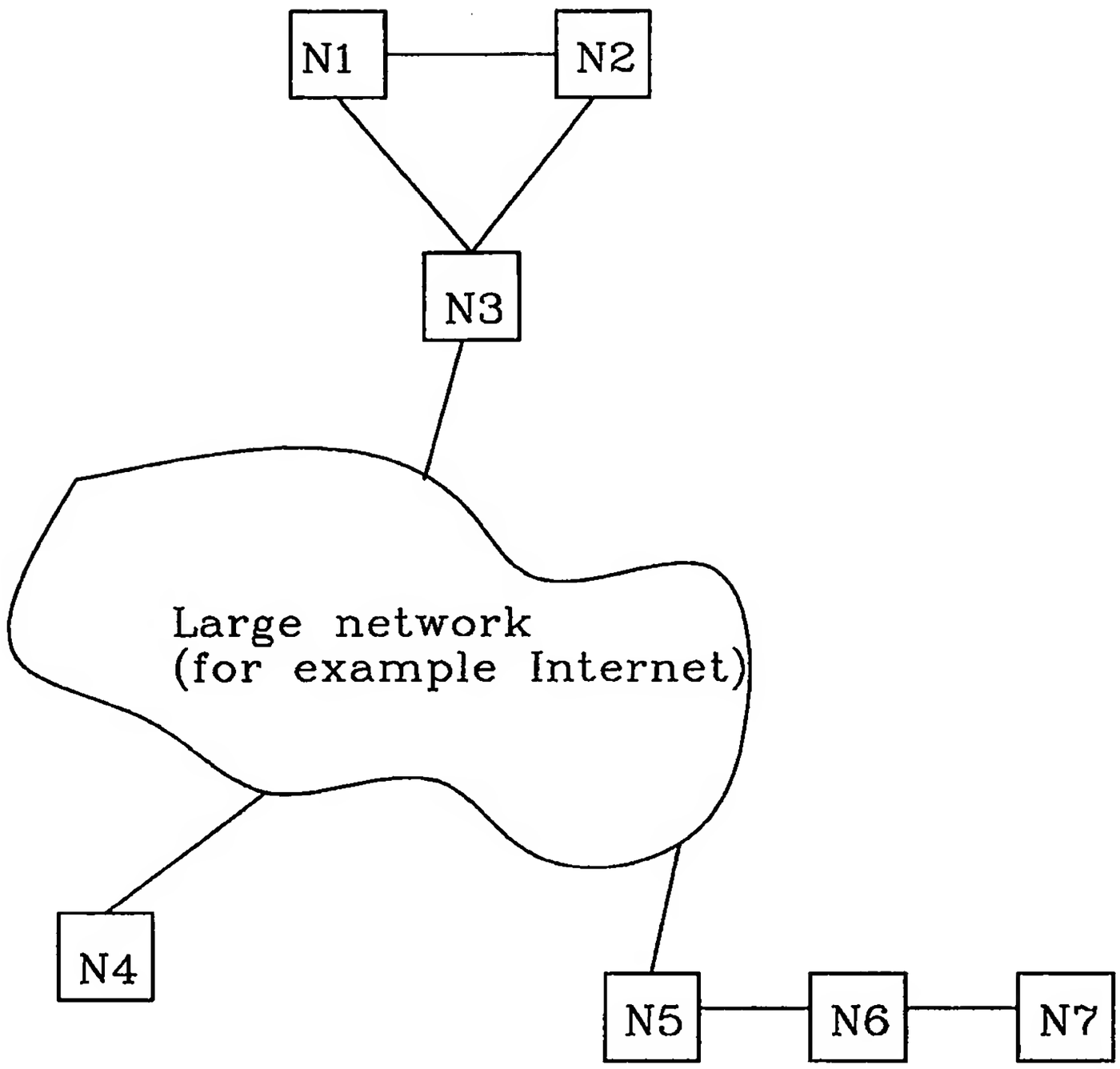


Fig.1

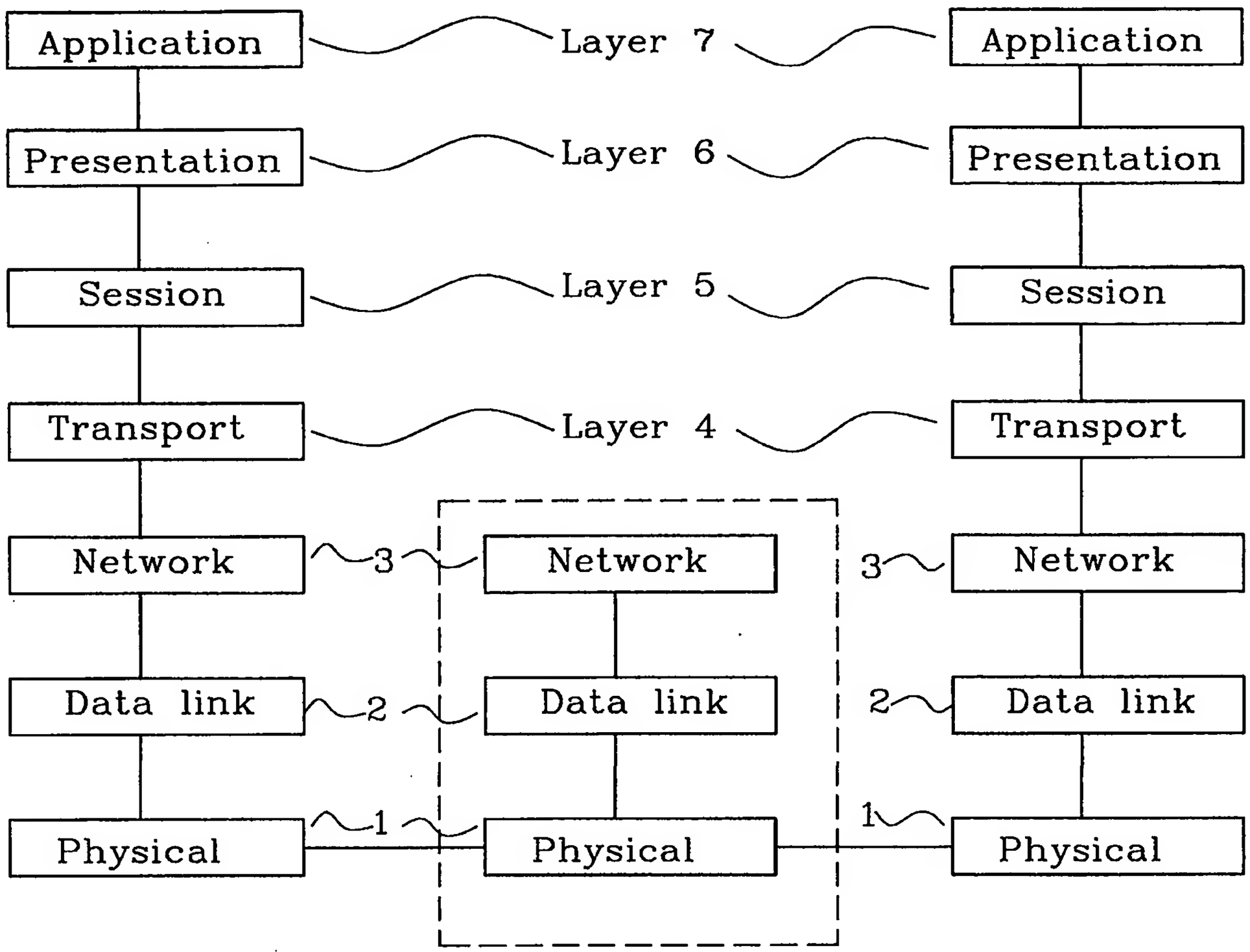

Application
Layer 7
Application
Presentation
Layer 6
Presentation
Session
Layer 5
Session
Transport
Layer 4
Transport
Network
3
Network
3
Network
Data link
2
Data link
2
Data link
Physical
1
Physical
1
Physical
One or more
nodes within
the network

Fig.2

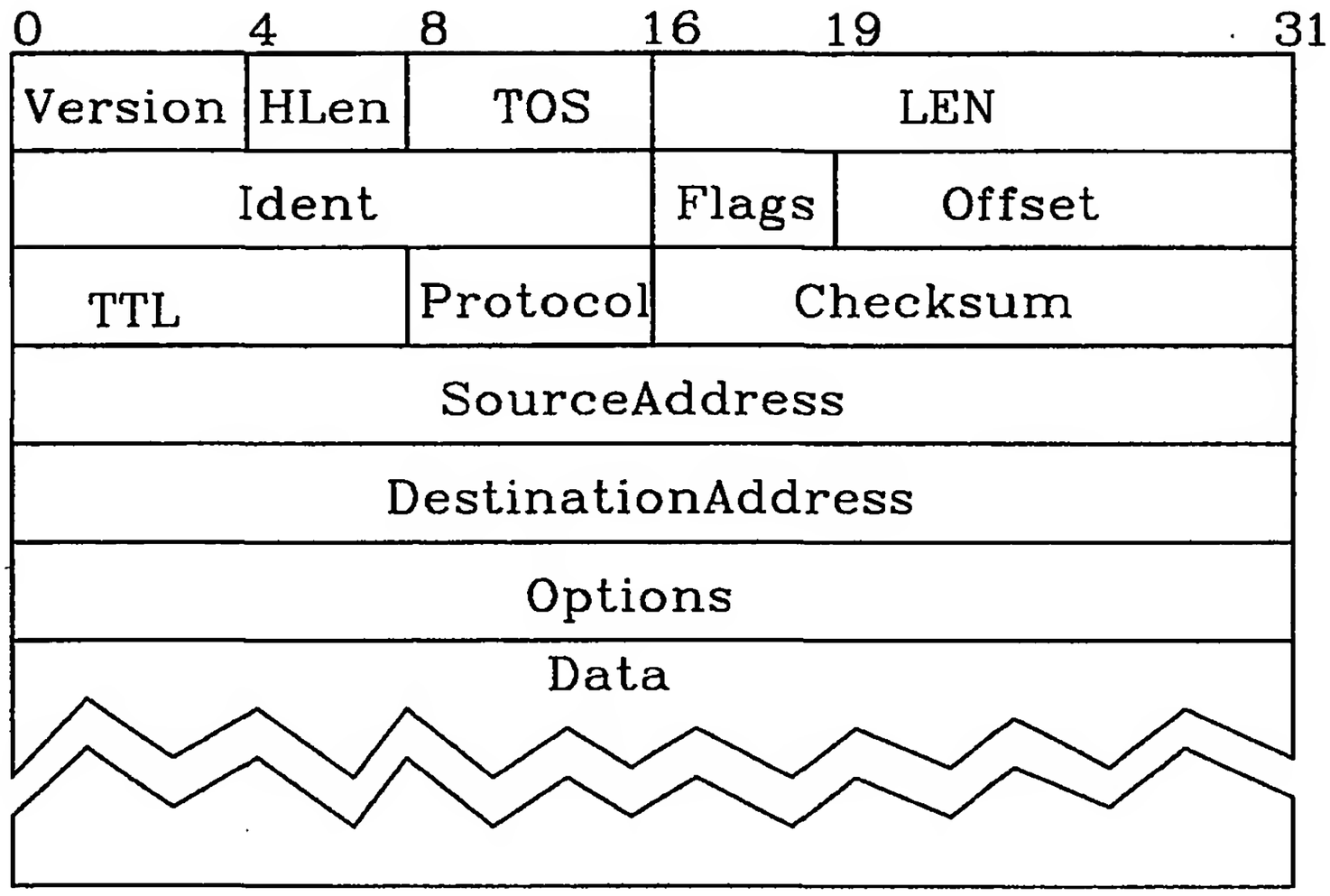

0
4
8
16
19
31
Version
HLen
TOS
LEN
Ident
Flags
Offset
TTL
Protocol
Checksum
SourceAddress
DestinationAddress
Options
Data

Fig.3

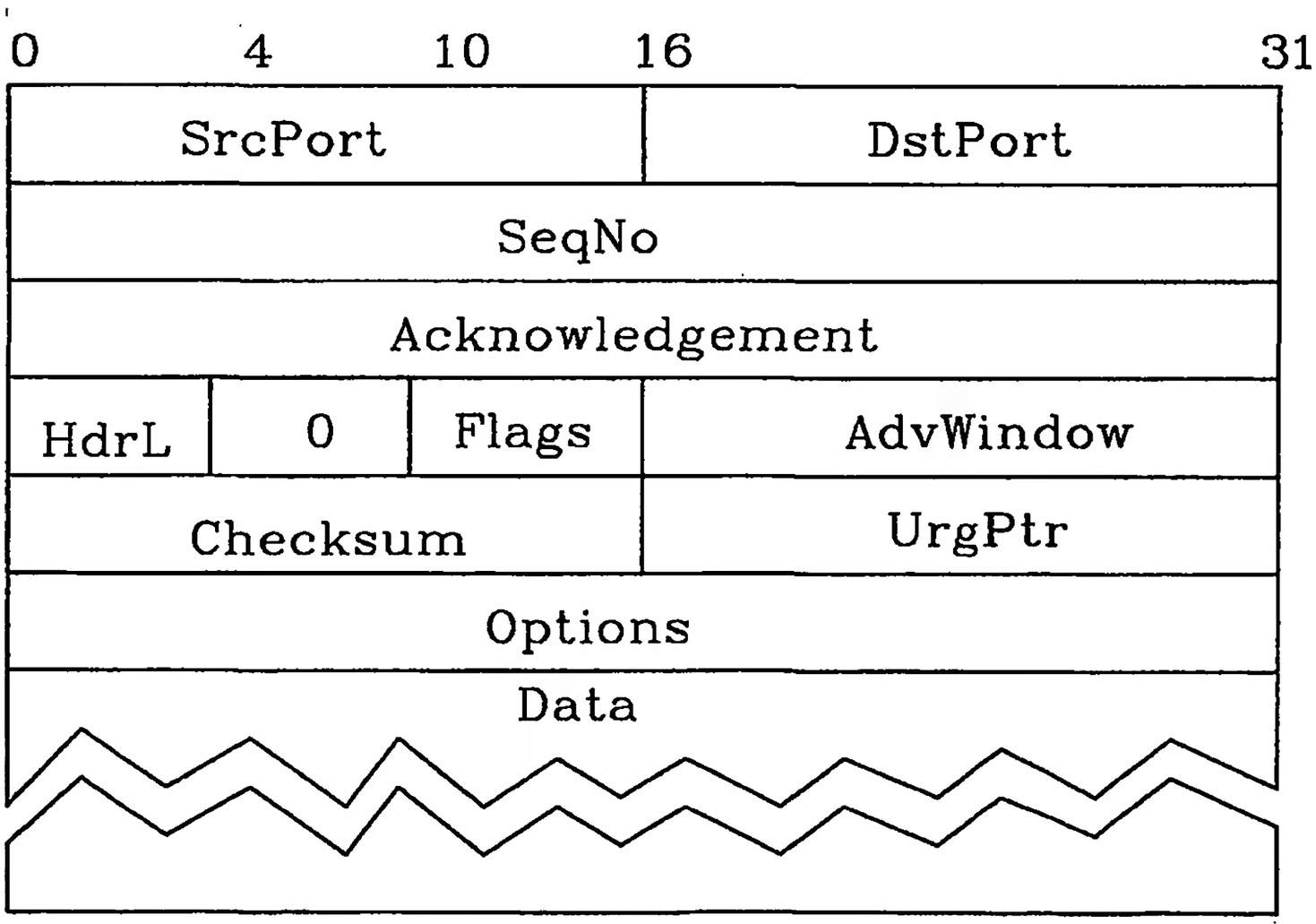

0
4
10
16
31
SrcPort
DstPort
SeqNo
Acknowledgement
HdrL
0
Flags
AdvWindow
Checksum
UrgPtr
Options
Data

Fig.4

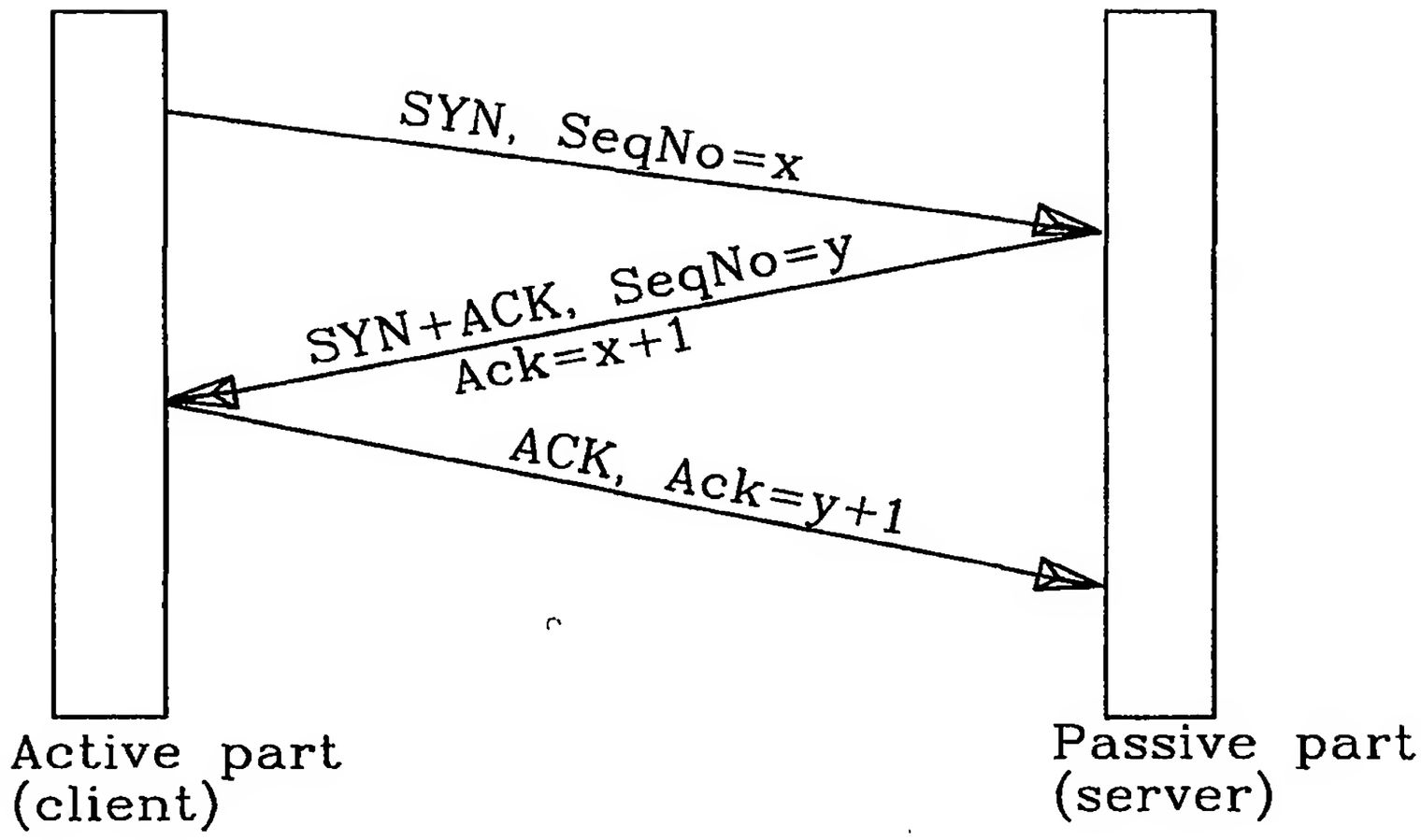

SYN, SeqNo=x
SYN+ACK, SeqNo=y
Ack=x+1
ACK, Ack=y+1
Active part
(client)
Passive part
(server)

Fig.5

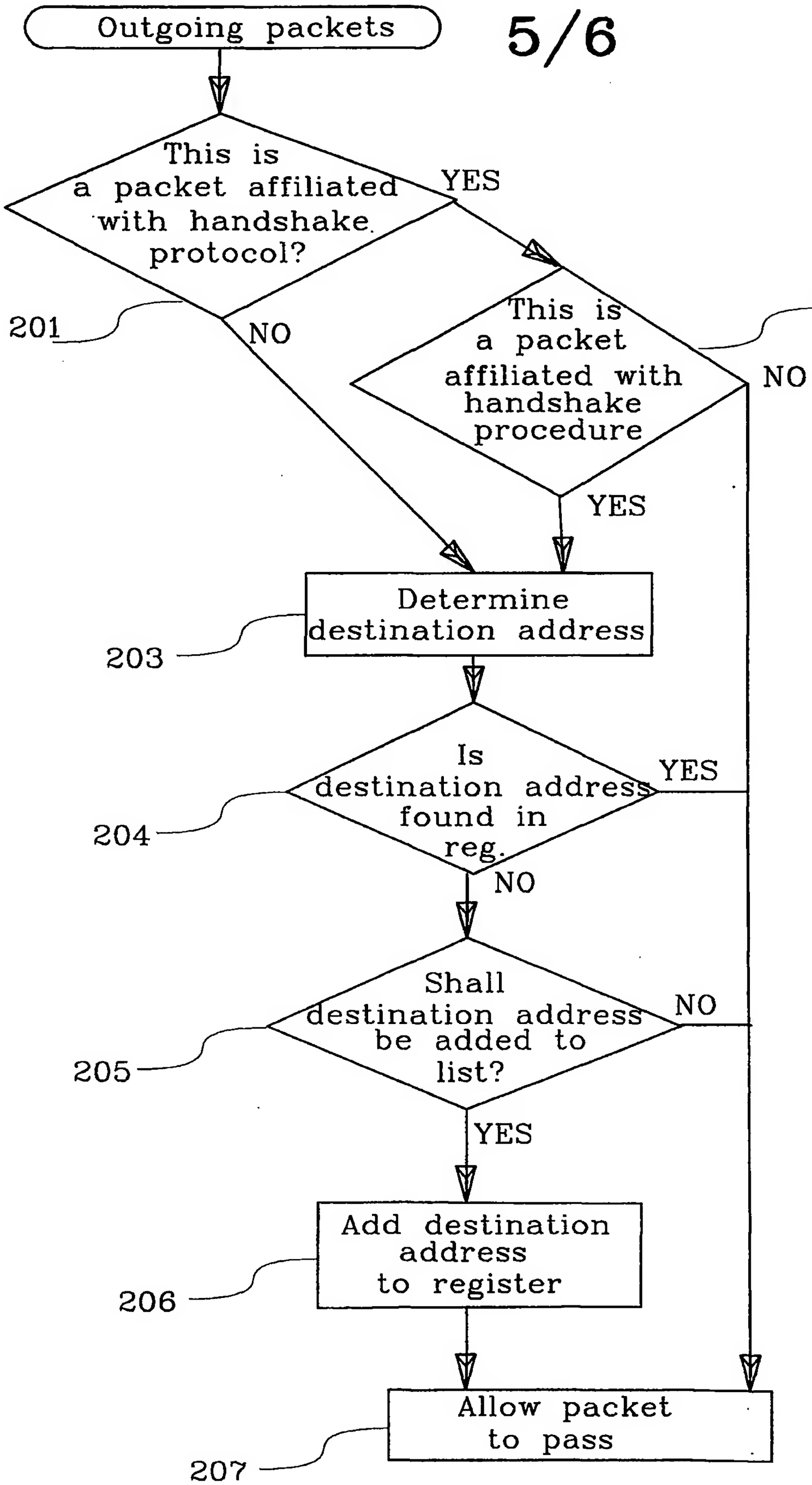

Outgoing packets
This is a packet affiliated with handshake protocol?
YES
NO
201
This is a packet affiliated with handshake procedure
202
NO
YES
Determine destination address
203
Is destination address found in reg.
204
YES
NO
Shall destination address be added to list?
205
NO
YES
Add destination address to register
206
Allow packet to pass
207

Fig.6

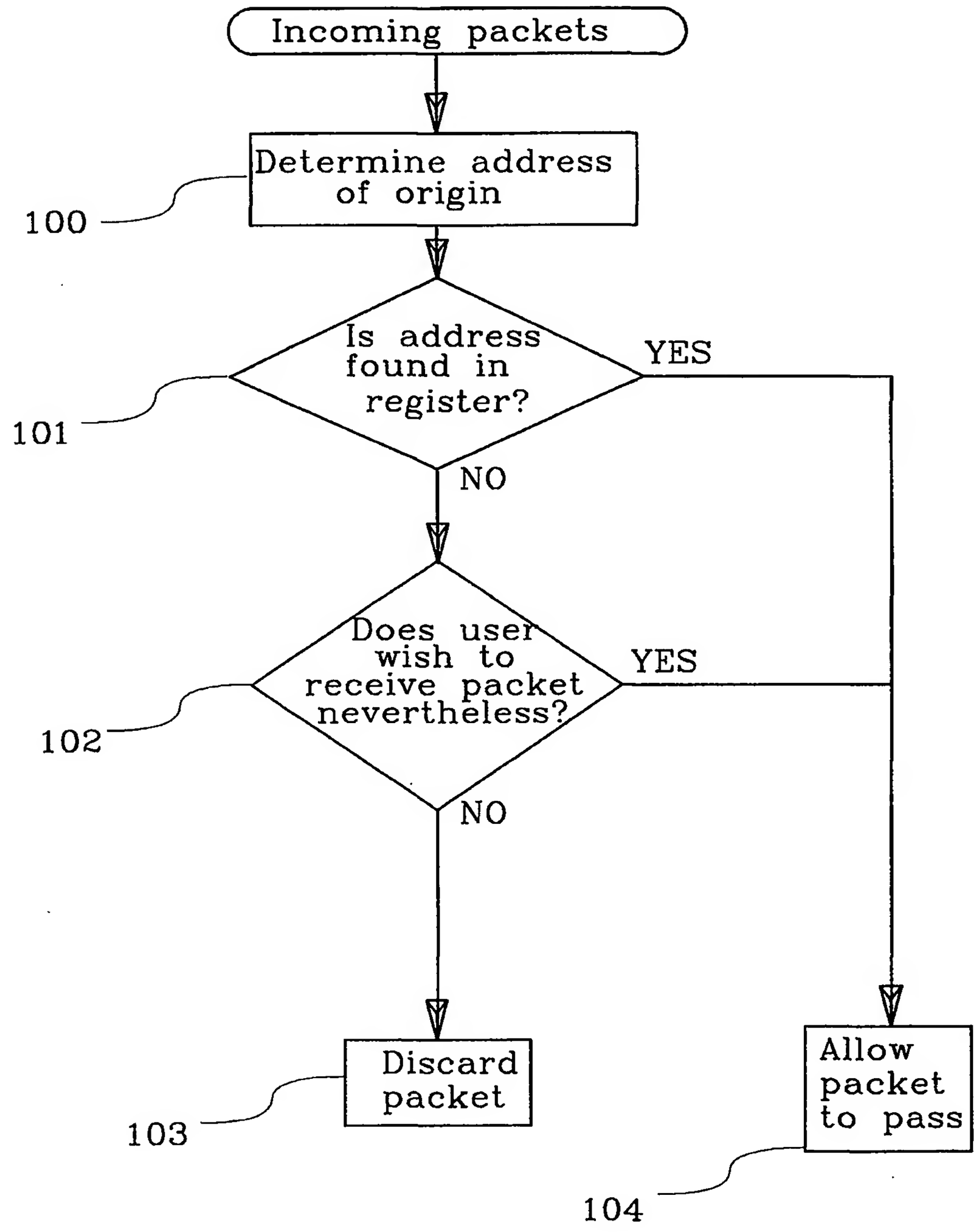

Incoming packets
Determine address of origin
100
Is address found in register?
101
YES
NO
Does user wish to receive packet nevertheless?
102
YES
NO
Discard packet
103
Allow packet to pass
104

Fig.7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01590

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 29/06, H04Q 11/04
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI DATA, EPO-INTERNAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9959071 A1 (MOTOROLA INC), 18 November 1999 (18.11.99), page 3, line 25 - line 31; page 5, line 11 - line 29; page 7, line 7 - line 16, claim 7 --	1-21
X	WO 9921340 A1 (AT&T WIRELESS SERVICES, INC), 29 April 1999 (29.04.99), page 12, line 19 - line 25, abstract --	1-21
X	EP 0873038 A2 (ALCATEL ALSTHOM COMPAGNIE GENERALE D'ELECTRIC), 21 October 1998 (21.10.98), column 7, line 4 - line 39 --	1-21

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 October 2001	17 -10- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM	Authorized officer

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 01/01590

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9812840 A1 (CABLETRON SYSTEMS, INC), 26 March 1998 (26.03.98), claim 19 ---	1,14
A	US 5774552 A (GRIMMER, F.), 3 June 1998 (03.06.98), column 1, line 48 - line 63; column 5, line 29 - line 53 ---	1,14
A	US 5996011 A (HUMES, D.), 30 November 1999 (30.11.99), column 2, line 5 - line 21 --- ---	1-21

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SE 01/01590

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9959071 A1	18/11/99	CN 1308745 T	15/08/01
		EP 1088261 A	04/04/01
		US 6132748 A	17/10/00
		US 6189035 B	13/02/01
WO 9921340 A1	29/04/99	US 6092110 A	18/07/00
EP 0873038 A2	21/10/98	AU 6070798 A	15/10/98
		AU 6070898 A	15/10/98
		AU 6812498 A	30/10/98
		AU PO610597 D	00/00/00
		CA 2231039 A	09/10/98
		CA 2231047 A	09/10/98
		CA 2231217 A	09/10/98
		EP 0884925 A	16/12/98
		EP 0974218 A	26/01/00
		JP 3188866 B	16/07/01
		JP 11032059 A	02/02/99
		JP 11041272 A	12/02/99
		JP 11055330 A	26/02/99
		US 6189042 B	13/02/01
		WO 9845995 A	15/10/98
		AU PO643197 D	00/00/00
WO 9812840 A1	26/03/98	AU 4425697 A	14/04/98
		EP 0927475 A	07/07/99
US 5774552 A	03/06/98	EP 0782296 A	02/07/97
		JP 9219701 A	19/08/97
US 5996011 A	30/11/99	NONE	